Alice P. Frazier, Chair
Michael J. Burke, Jr., Chairman-Elect
Shon B. Myers, Vice Chairman
Jill Sung, Treasurer
Douglas E. Parrott, Secretary
Jack E. Hopkins, Immediate Past Chairman
Rebeca Romero Rainey, President and CEO

June 09, 2026

Regulatory and Strategic Affairs Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

RE: Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, [Docket No. FINCEN–2026–0100] RIN 1506–AB73

Dear Sir or Madam:

The Independent Community Bankers of America ("ICBA")[1] appreciates the opportunity to comment on the joint proposed rule issued by the Financial Crimes Enforcement Network ("FinCEN") and the Office of Foreign Assets Control ("OFAC") to implement the anti-money laundering/countering the financing of terrorism ("AML/CFT") and sanctions compliance provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act ("GENIUS Act").[2] The proposal would treat permitted payment stablecoin issuers ("PPSIs") as financial institutions ("FI"s) for Bank Secrecy Act ("BSA") purposes and would require them to maintain AML/CFT programs, comply with core reporting and recordkeeping obligations, and adopt effective sanctions compliance programs.[3]

ICBA strongly supports a federal illicit-finance framework for PPSIs that is no weaker than the framework applicable to community banks. Community banks already operate under extensive AML/CFT, sanctions, examination, audit, and reporting obligations, and nonbank issuers offering bank-like payment products should not be permitted to compete under materially weaker standards. ICBA has long warned that stablecoins can facilitate illicit finance, including as an "underground banking" channel for crypto scam operators and as a sanctions-evasion tool for actors tied to Russia, Iran, and North Korea. Treasury should therefore adopt a final rule that closes these regulatory gaps, curbs regulatory arbitrage, and ensures that payment stablecoin activity does not develop under weaker protections for consumers, law enforcement, or the broader financial system.

Background

Payment stablecoins emerged to address a fundamental limitation of early digital assets: extreme price

[1] The Independent Community Bankers of America® has one mission: to create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovative offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams. For more information, visit icba.org.
[2] Guiding and Establishing National Innovation for U.S. Stablecoins Act, 12 U.S.C. §§ 5901–5916 (2025).
[3] Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions-Compliance Program Requirements, 91 Fed. Reg. 18,360 (proposed Apr. 10, 2026) (to be codified at 31 C.F.R. ch. X and V)

volatility that made them poorly suited for routine payments and settlement. But as stablecoins grew alongside the broader crypto market, they became not only the principal instrument for crypto asset trading, but also a significant channel through which illicit actors can move value quickly, globally, and with reduced transparency. As of June 2026, nearly four hundred stablecoins collectively account for approximately $320 billion in value, with the market heavily concentrated in Tether/USDT ($187 billion) and Circle's USDC ($76 billion).[4]

Those features that make stablecoins attractive for legitimate market activity—price stability, high liquidity, rapid settlement, and broad cross-border usability—also make them particularly attractive to cybercriminals, fraud networks, sanctions evaders, and other illicit actors. Stablecoins can be transferred near instantaneously across borders, including to and from sanctioned jurisdictions, and can be held through vast numbers of unhosted wallets that are not subject to customer identification or AML controls. In addition, fragmented and underdeveloped regulatory regimes have created opportunities for bad actors to exploit gaps in oversight, attribution, and enforcement. As the Multilateral Sanctions Monitoring Team has warned, this combination of capabilities has provided DPRK-linked actors with a new method to circumvent sanctions programs, including through the use of USDT as a payment mechanism that "is less cumbersome and safer than cash transactions."[5]

Recent data underscore the scale and urgency of these risks. Chainalysis reports that illicit cryptocurrency addresses received at least $154 billion in 2025, a 162 percent year-over-year increase due to a nearly 700 percent surge in value received by sanctioned individuals.[6] The same report found that stablecoins accounted for 84 percent of all illicit cryptocurrency transaction volume, underscoring how central they have become to modern illicit-finance activity.[7] These trends should not be treated as isolated warning signs or temporary market distortions. They demonstrate that stablecoins already present material money laundering, sanctions-evasion, and national-security risks that warrant a rigorous federal regulatory response.

Congress responded to these realities by enacting the GENIUS Act, which establishes a federal framework for payment stablecoin issuance and generally limits issuance in the United States to PPSIs subject to federal or qualifying state supervision. The statute also directs Treasury to treat PPSIs as financial institutions for purposes of the Bank Secrecy Act and to impose AML/CFT and sanctions compliance obligations on those entities. That directive reflects a sound and necessary judgment: where a payment product can move value rapidly, pseudonymously, and across borders with limited visibility into counterparties or downstream transfers, the regulatory framework should be at least as strong as the framework that applies to comparable activity in the banking system.

Following enactment, Treasury initiated a rulemaking process to implement those statutory mandates into operational requirements for payment stablecoin activity. Treasury's September 2025 Advance Notice of Proposed Rulemaking sought input on key implementation questions, including the scope of

---

[4] *Stablecoins*, DeFiLlama, https://defillama.com/stablecoins (last visited May 28, 2026).
[5] Multilateral Sanctions Monitoring Team, *The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities* 51 (Oct. 22, 2025), https://msmt.info/Publications/Reports
[6] *2026 Crypto Crime Report Introduction: Crypto Crime Reaches Record High in 2025 as Nation-State Sanctions Evasion Moves On-Chain at Scale*, Chainalysis (Jan. 8, 2026), https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/.
[7] *Id.*

Bank Secrecy Act coverage, the application of the Travel Rule in on-chain contexts, and the balance between federal and state supervision. As Treasury moves to finalize this rulemaking, it should do so with appropriate caution: any gaps, ambiguities, or premature accommodations in the final framework could be exploited by actors seeking to use stablecoin structures to circumvent controls that would apply in more traditional financial channels. Moreover, Treasury should approach claims that stablecoin activity warrants lighter treatment with substantial skepticism, particularly where technological design choices reduce visibility, impede attribution, or weaken the practical ability to detect and stop illicit activity.

Interagency coordination has been central to the implementation effort. Treasury and OFAC have worked in tandem to craft a proposed rule that addresses both AML/CFT program expectations and sanctions compliance obligations. The joint proposed rule is therefore the product of statutory direction, public consultation, and interagency coordination.

Executive Summary

ICBA supports Treasury's effort to establish a federal AML/CFT and sanctions framework for PPSIs. As the proposed rule recognizes, payment stablecoins may offer enhanced payment capabilities, but the strength, size, and reliability of the U.S. financial system also make these systems a notable target for misuse by illicit actors, with consequences for U.S. national security.[8] Treasury should therefore adopt a final rule that is rigorous, enforceable, and designed to ensure that payment stablecoin activity does not operate under weaker standards than comparable payment activity conducted through community banks. ICBA's principal recommendations are summarized below.

- Treasury should adopt a strong federal illicit-finance framework for PPSIs and make clear that nonbank issuers offering bank-like payment products will not be permitted to operate under weaker standards than community banks.
- Treasury should require PPSIs to meet robust AML/CFT and sanctions obligations and should reject any tailoring or exemptions that would dilute core compliance safeguards.
- Because stablecoin activity can obscure counterparties, ownership, and downstream transfers, Treasury should impose strict and enforceable obligations.
- Treasury should establish clear reporting, recordkeeping, and information-sharing rules and should not create exemptions until equivalent transparency and enforcement value are affirmatively proven.
- OFAC should require PPSIs to maintain fully effective sanctions programs, clear lawful-order compliance obligations, and credible block, freeze, and reject capabilities.
- Treasury should extend or phase in implementation if related stablecoin rules remain unresolved or core compliance expectations are not yet sufficiently clear to support sound implementation.

ICBA's Comments

Treatment of Permitted Payment Stablecoin Issuers as Financial Institutions Under the Bank Secrecy Act

[8] Permitted Payment Stablecoin Issuer AML/CFT Program and Sanctions-Compliance Program Requirements, 91 Fed. Reg. at 18582.

The proposed rule would implement the GENIUS Act's directive that PPSIs be treated as financial institutions for purposes of the Bank Secrecy Act and, accordingly, be subject to AML/CFT, reporting, recordkeeping, and related compliance obligations. ICBA supports this approach. An entity that issues a payment instrument intended for broad transactional use should not fall outside the federal illicit-finance framework merely because the instrument is issued through a stablecoin structure rather than a traditional deposit or other conventional payment mechanism. Treasury's proposal appropriately recognizes that PPSIs should be treated as covered FIs under the BSA and held accountable for maintaining compliance systems commensurate with the risks presented by their activities.

This treatment is important not only as a matter of statutory implementation, but also as a matter of competitive equity and regulatory integrity. Community banks already operate under comprehensive Bank Secrecy Act, sanctions, examination, audit, and reporting requirements when providing payment services to their customers. PPSIs offering functionally comparable payment capabilities should not be permitted to compete in the same market under materially weaker or less certain standards. Allowing comparable payment activity to migrate outside the banking system without equivalent baseline obligations would create avoidable gaps in law-enforcement visibility, weaken accountability for illicit-finance controls, and create incentives for regulatory arbitrage. Treasury should therefore finalize a rule that clearly places PPSIs within the federal financial-institution framework rather than establishing a separate category of payment provider subject to diluted expectations.

ICBA recognizes that Treasury may tailor particular obligations to reflect the size, complexity, delivery channels, and operational model of a PPSI. Any such tailoring, however, should operate within a strong baseline of enforceable obligations and should not weaken the core responsibilities that accompany treatment as a FI under the BSA. At a minimum, PPSIs should be expected to maintain effective governance, risk assessment, customer due diligence, suspicious activity monitoring, recordkeeping, sanctions controls, and the operational capacity to comply with lawful orders and other applicable requirements. Although innovation in payment technology may warrant calibrated implementation, it does not justify exempting bank-like payment activity from the core federal framework designed to protect the financial system and support national security.

AML/CFT Program Requirements

Written AML/CFT Program

The proposed rule would require each PPSI to establish and maintain a written AML/CFT program. ICBA supports that requirement because a documented program is the foundation of effective compliance and is necessary to ensure that governance, customer due diligence, monitoring, escalation, suspicious activity review, recordkeeping, independent testing, and training are clearly defined, consistently implemented, and subject to meaningful oversight. For PPSIs, a written program is especially important because stablecoin activity may involve novel technology, layered intermediaries, rapid movement of value, and limited visibility into counterparties and downstream transactions. The final rule should therefore make clear that the written program must do more than restate high-level principles. It should set out the issuer's compliance responsibilities, internal controls, lines of authority, escalation procedures, use of third parties or service providers, and processes for updating controls as products, technology, and risks continue to evolve. Treasury should also make clear that a written program is not a check-the-box document but an enforceable framework for day-to-day compliance that can be evaluated through supervision and examination.

The proposed rule would require each PPSI to establish and maintain a written, risk-based anti-money laundering/countering the financing of terrorism program supported by internal controls, independent testing, designated compliance leadership, training, and customer due diligence procedures.[9] ICBA supports this requirement because these are core features of effective illicit-finance risk management, and they should apply whenever a firm offers a bank-like payment product, regardless of whether that product is delivered through traditional account relationships or digitally native stablecoin structures. We also support a final rule that requires PPSIs to maintain AML/CFT programs that are adequately resourced, tailored to the issuer's risks, and capable of identifying and addressing risks associated with wallet-based activity, rapid movement of value, layered intermediaries, and limited visibility into counterparties and downstream transfers. However, while a risk-based framework is appropriate, it should not permit weak governance, superficial controls, or ambiguity about who is responsible for monitoring, escalation, customer due diligence, suspicious activity review, and related core AML/CFT functions. A risk-based framework should not be used to justify weaker controls in place of robust compliance measures.

Risk Assessments

The proposed rule would require each PPSI to maintain a written, risk-based AML/CFT program.[10] FinCEN would also require PPSIs to update their risk assessments promptly whenever they know, or have reason to know, that there has been a significant change in their risk profile.[11]

ICBA has long supported a risk-based approach that gives community banks appropriate flexibility to tailor risk assessments to their size, complexity, business model, customer base, and delivery channels. In the community bank context, that flexibility is important because effective compliance depends on calibrating controls to actual risk rather than imposing a one-size-fits-all framework that may not reflect how a particular institution operates. But PPSIs present a different case. Because the proposed rule applies to a digitally native payment product that may move rapidly across wallets, intermediaries, exchanges, and various secondary-market channels, including decentralized protocols, Treasury should make clear that flexibility in this context cannot rest on the same assumptions that often apply to more traditional banking models. PPSIs should be required to conduct documented, periodically updated risk assessments that address not only traditional customer, product, geographic, and transactional risks, but also stablecoin-specific factors such as wallet architecture, issuance and redemption channels, intermediary and custodial arrangements, on-chain and off-chain activity, secondary-market exposure, cross-border transfer patterns, sanctions-related risk, and the degree to which the issuer has visibility into counterparties and downstream movement of value. That analysis is necessary because stablecoin activity can fragment responsibility, complicate attribution, and weaken the transaction visibility on which many traditional monitoring models depend.

Treasury should therefore impose a clear and more robust review and update requirement. At a minimum, PPSIs should be required to review risk assessments on a regular schedule and to revise them whenever material changes occur in the issuer's products, token design, technology stack, governance, customer base, geographic footprint, distribution channels, intermediary relationships,

[9] *Id.* at 18582-18583.
[10] *Id.* at 18598.
[11] *Id.*

sanctions exposure, or transaction typologies. Updates also should be required after significant compliance incidents, audit findings, enforcement developments, suspicious activity trends, or other events that call prior risk assumptions into question. Those revisions should occur without unreasonable delay and early enough to support interim controls, escalation decisions, management action, and any necessary changes to monitoring, due diligence, or reporting before the relevant risk becomes embedded in ongoing operations.

The final rule should also make clear that risk assessments are not static documents prepared for onboarding or examination purposes; instead, they are living compliance tools that must be used to recalibrate governance, customer due diligence, monitoring rules, escalation protocols, recordkeeping, testing, staffing, and control design as the issuer's risks evolve. Although AML/CFT and sanctions risk assessments may be coordinated where appropriate, the final rule should make clear that PPSIs remain responsible for conducting a sufficiently robust assessment of illicit-finance risk rather than relying on broad assumptions, generic templates, or enterprise-level analyses that do not capture the distinct features of stablecoin activity.

Designation and Duties of an AML/CFT Officer

The proposed rule would require PPSIs to designate a qualified individual responsible for establishing and implementing the AML/CFT program and for coordinating and monitoring day-to-day compliance with the BSA.[12] ICBA supports this requirement and agrees that the effectiveness of a PPSI's AML/CFT program depends fundamentally on the authority, independence, and resourcing of the designated AML/CFT officer.

At the same time, Treasury should make clear that, in the PPSI context, qualification for this role requires more than general compliance experience. Given the unique characteristics of stablecoin activity—including wallet-based transactions, rapid cross-border transfers, layered intermediaries, smart contract execution, and limited visibility into counterparties and downstream transfers—an AML/CFT officer must possess demonstrated expertise in digital asset markets, blockchain-based payment systems, and stablecoin-specific risk typologies. Absent that specialized knowledge, the officer may lack the practical ability to identify, assess, and mitigate the risks inherent in PPSI operations.

Accordingly, the final rule should clarify that a PPSI's AML/CFT officer must have sufficient technical, operational, and risk management knowledge of the issuer's token design, wallet architecture, issuance and redemption processes, and transaction flows across both primary and secondary markets. This includes an understanding of how stablecoins may be used in practice to facilitate illicit finance, including through decentralized platforms, unhosted wallets, cross-chain transfers, or intermediary layering that can obscure ownership and control.

ICBA agrees that the rule should focus on the officer's functional authority and organizational stature rather than formal title.[13] However, Treasury should also emphasize that the AML/CFT officer must be embedded within, and actively engaged in, the PPSI's product design, governance, and operational

[12] *Id.* at 18601.
[13] *Id.*

decision-making processes. Because design choices—such as wallet architecture, smart contract functionality, or intermediary arrangements—can directly affect compliance outcomes, the AML/CFT officer must have meaningful input into those decisions to ensure that compliance capabilities are built into the system rather than applied afterwards.

With respect to resources, ICBA supports Treasury's emphasis on adequate staffing, funding, and technology.[14] In the PPSI context, these resources must include specialized compliance personnel with expertise in blockchain analytics, transaction tracing, and sanctions screening in digital environments, as well as technological systems capable of monitoring activity across on-chain and off-chain environments. Treasury should clarify that resource adequacy must be evaluated not only in relation to traditional factors such as size and complexity, but also in light of the velocity, opacity, and cross-border nature of stablecoin transactions, which may require more advanced monitoring and investigative capabilities than those used in traditional account-based banking.

FinCEN states that the individual serving as the AML/CFT officer must be qualified for that role and not overburdened with other responsibilities at the institution.[15] The proposed rule further provides that an AML/CFT officer with conflicting responsibilities that adversely affect the officer's ability to coordinate and monitor day-to-day AML/CFT compliance generally would not satisfy this requirement.[16] ICBA has long recognized that, in the community bank context, BSA/AML officers often perform multiple functions and that overlapping responsibilities do not automatically render an officer unqualified or ineffective. The PPSI context, however, warrants a different response. Because product design, wallet architecture, intermediary arrangements, and growth incentives can directly shape a PPSI's AML/CFT risk profile, Treasury should make clear that conflicting responsibilities in this context include not only competing time demands, but also structural and organizational conflicts that may undermine the officer's independence from product, engineering, or revenue-generating functions. A PPSI should not be permitted to structure its operations in a manner that limits the AML/CFT officer's ability to challenge product design, escalate risk, or require changes necessary to support compliance with BSA and sanctions obligations.

Proposed Additional Technical Capabilities

The proposed rule would require PPSIs to maintain the technical capability to block, freeze, and reject transactions, as necessary.[17] ICBA supports that requirement. Treasury should not dilute this core expectation simply because stablecoin activity may occur through novel technological designs or fragmented transaction chains. On the contrary, the speed, cross-border reach, and transferability of stablecoins make effective intervention capabilities especially important. If value can move rapidly across wallets, intermediaries, smart contracts, or platforms with limited visibility into the identity of the transacting parties or the downstream destination of funds, then the need for prompt, enforceable blocking and freezing capabilities becomes more critical.
ICBA recognizes that PPSIs may face technical and operational challenges in implementing these capabilities, including questions regarding wallet architecture, token design, control over smart contract functionality, the role of intermediaries, treatment of omnibus or custodial arrangements, and the extent to which an issuer can act effectively once tokens move into secondary-market circulation. But those

[14] *Id.*
[15] *Id*.
[16] *Id.*
[17] *Id.* at 18617

challenges should not become a basis for weaker obligations or open-ended flexibility. A firm that chooses to issue a bank-like payment instrument using technology that limits its ability to identify relevant actors or intervene when required should not be permitted to operate under a reduced sanctions standard as a result of that design choice. Treasury should instead require PPSIs to build products, governance, contractual arrangements, and compliance systems that support timely execution of block, freeze, and reject functions, and should provide sufficiently clear guidance regarding what constitutes an effective capability in different transaction environments. Any implementation flexibility should be narrow, operationally justified, and designed to support compliance—not to excuse gaps in enforceability, create uncertainty for counterparties and examiners, or allow stablecoin activity to proceed under materially weaker controls than those that apply to community banks offering functionally similar payment services.

Scope of Compliance Obligations for Primary and Secondary Market Activity

Under the Proposal, the agencies draw a sharp distinction between the primary market—where a PPSI has a direct relationship with the user—and the secondary market, where payment stablecoins circulate beyond that direct relationship through unhosted and hosted wallets and decentralized protocols.[18] FinCEN itself acknowledges that "the majority of illicit activity involving stablecoins occurs on the secondary market."[19] Yet despite that finding, FinCEN would neither require PPSIs to monitor secondary market activity nor to file Suspicious Activity Reports ("SARs") related to it.[20] FinCEN reasons that the burden of requiring such reporting could outweigh the benefits.[21]

ICBA and its members are deeply concerned about this approach. First, given the significant and growing use of stablecoins in illicit finance—including sanctions evasion—FinCEN should not disclaim responsibility for the portion of the market it identifies as presenting the greatest risk. Although FinCEN expresses concern that reporting obligations could generate unwarranted filings and complicate detection efforts, the complete absence of any monitoring or SAR expectation risks leaving significant illicit activity unchecked. Recent OFAC enforcement further underscores that sanctions compliance cannot be confined to formal direct relationships or a narrow view of who is immediately transacting with whom. As OFAC recently emphasized, it is prohibited to do indirectly what one cannot do directly, and transacting through another party does not make otherwise prohibited conduct permissible.[22] That principle is directly relevant here. If PPSIs design products, distribution models, or intermediary arrangements that permit sanctioned persons or other illicit actors to access stablecoin functionality indirectly through secondary-market channels, those structures should not be treated as outside the

practical reach of sanctions compliance merely because the issuer lacks a direct primary-market relationship with the end user.

Second, FinCEN's proposed approach may create a regulatory gap at precisely the wrong moment.

---

[18] I*d.* at 18592.
[19] I*d.* at 18601.
[20] I*d.* at 18592.
[21] *Id.*
[22] U.S. Dep't of the Treasury, Off. of Foreign Assets Control, *FTI Consulting, Inc., a Global Business Advisory Firm, Settles with OFAC for $1,050,000 Related to Apparent Violations of Dealing in Prohibited Debt of Sanctioned Russian Bank* (June 1, 2026).

Depending on how Congress resolves key questions in legislation such as the Digital Asset Market Clarity Act of 2025,[23] some stablecoin activity could fall outside a clear regulatory framework altogether. If decentralized finance continues to expand, transactions involving unhosted wallets, decentralized exchanges, and cross-chain bridges may evade meaningful oversight. Considering ongoing congressional debate over AML/KYC obligations across the crypto ecosystem, it is premature for FinCEN to conclude that PPSIs should bear no responsibility with respect to the secondary market.

Finally, ICBA cautions that exempting PPSIs from secondary market monitoring and reporting obligations could produce materially different regulatory treatment for payment stablecoins and tokenized deposits. Although the regulatory framework for tokenized deposits remains uncertain, if tokenized deposit issuers ultimately face a more stringent and costly regime, the result could be an uneven playing field that advantages PPSIs. While FinCEN and OFAC are not charged with addressing financial stability, their rules could accelerate the growth of payment stablecoins and contribute to the disintermediation of deposits from community banks and a corresponding decline in credit availability for small businesses, farmers, and rural communities.

Reporting, Recordkeeping, and Information Sharing Requirements

The proposed rule would apply core reporting, recordkeeping, and information-sharing requirements to PPSIs as covered financial institutions. ICBA supports applying these requirements because they are foundational tools for detecting illicit finance and supporting investigations. That said, FinCEN should recognize that stablecoin activity can present materially different visibility challenges from traditional account-based banking. In many cases, the issuer or intermediary may have only partial visibility into the identity of the transacting parties, the beneficial owner behind a wallet, the purpose of a transfer, the role of intermediaries, or the downstream movement of tokens after initial issuance or redemption. These gaps are especially pronounced where activity occurs through unhosted wallets, omnibus arrangements, layered intermediaries, smart contracts, secondary-market transfers, or cross-border blockchain-based movement of value. For that reason, Treasury should provide clearer guidance on how the Recordkeeping Rule and Travel Rule apply across different transaction structures, intermediaries, and technological environments.

Stablecoin transaction chains may involve multiple parties performing fragmented functions, which can make it difficult to determine who must collect, retain, verify, or transmit required information and at what point in the transaction flow. Wallet addresses alone do not necessarily provide meaningful information about the person or entity controlling the transaction, and blockchain transparency does not eliminate the practical difficulty of attributing on-chain activity to real-world actors or understanding the commercial purpose of a transfer. The final rule should therefore provide sufficient clarity so that issuers, counterparties, and examiners have a common understanding of what information must be collected, how far obligations extend into secondary-market activity, when reliance on intermediaries is permissible, and how compliance expectations apply where full visibility is not realistically available.

---

[23] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Cong. § 1(a) (2025). (establishing a comprehensive federal framework for the regulation of digital assets, including allocation of jurisdiction between the Securities and Exchange Commission and Commodity Futures Trading Commission and creation of registration requirements for digital asset intermediaries).

ICBA further supports extending appropriate information-sharing tools, including provisions equivalent to sections 314(a)[24] and 314(b)[25] of the USA PATRIOT Act, to PPSIs. Expanded information-sharing is especially important in a market where no single participant may have complete visibility into the full lifecycle of a stablecoin transaction. But information-sharing authorities will be materially less effective if PPSIs are not assigned clear underlying responsibilities to collect, retain, and be able to provide relevant customer, transaction, wallet, and counterparty information in the first instance. If a PPSI is permitted to operate without meaningful obligations to identify relevant parties, maintain records, monitor activity, or preserve information about issuance, redemption, transfers, intermediaries, or wallet-linked relationships, then other financial institutions and law enforcement may have little useful information to request, compare, or share. In that scenario, fragmented transaction chains would not simply create visibility challenges—they would undermine the effectiveness of the information-sharing framework itself. Effective illicit finance controls therefore depend not only on the legal availability of information-sharing channels, but also on clear responsibility rules that require PPSIs to generate and maintain the information necessary to make those channels useful.

Currency Transaction Reporting

FinCEN proposes applying CTR obligations to PPSIs and asks whether to allow them to utilize the exemption process.[26]

ICBA strongly supports imposing CTR obligations on PPSIs to the extent those issuers engage in transactions or transaction structures that present functional cash-like risks or otherwise implicate the purposes served by such reporting. FinCEN should not create a regime in which nonbank issuers can offer bank-like payment products while avoiding core reporting obligations that community banks must satisfy when conducting functionally similar activity. Failing to apply appropriate reporting requirements would create an avoidable gap in the illicit finance framework, weaken law-enforcement visibility into potentially suspicious flows of value, and invite migration of activity into stablecoin channels precisely because those channels may be perceived as less transparent or less tightly regulated. That risk is particularly acute where stablecoin structures permit rapid movement of value, cross-border transfers, wallet-to-wallet activity, intermediary layering, or conversion pathways that can be used to obscure the source, destination, or purpose of funds. Treasury should therefore adopt a strong baseline expectation that PPSIs must support reporting where the underlying activity creates equivalent law-enforcement and anti-money laundering concerns, while providing clear guidance on how those obligations apply in practice.

ICBA opposes exemptions from CTR obligations unless and until FinCEN has determined, based on real operational evidence and supervisory experience, that effective CTR compliance can be achieved without creating material gaps in transparency, enforcement utility, or anti-evasion safeguards. Premature exemptions would risk undermining the purpose of the reporting regime before regulators have sufficient experience to assess how stablecoin transaction structures function in practice, how readily activity can be traced to real-world actors, and whether alternative controls are truly comparable. Treasury should begin from a presumption against exemptions until a PPSI can demonstrate that

[24] 31 C.F.R. § 1010.520 for section 314(a)
[25] 31 C.F.R. § 1010.540 for section 314(b)
[26] 91 Fed. Reg. at 18606

alternative controls provide equivalent transparency, traceability, and enforcement value. Thereafter, any exemption should be narrow, well-justified, and supported by a demonstrated record that will not weaken law-enforcement visibility, encourage structuring, or create materially weaker transparency requirements than those imposed on community banks.

Suspicious Activity Reports

This proposed rule would promulgate a requirement that PPSIs file SARs for any suspicious transaction.[27] FinCEN expects that requiring PPSIs to report suspicious activity would similarly provide highly useful information for investigations and proceedings involving domestic and international money laundering, terrorist financing, and other illicit finance activity, as well as for intelligence purposes.

ICBA strongly supports requiring PPSIs to file SARs because such reporting is one of the most important tools available to law enforcement and national security agencies for identifying illicit finance and connecting fragmented activity across institutions and channels. That obligation is especially important in the stablecoin context, where activity may move rapidly across wallets, platforms, intermediaries, and borders in ways that can outpace traditional account-based monitoring and reduce visibility into the identities of transacting parties, the purpose of transfers, and the downstream movement of funds after issuance or redemption. A PPSI may not have complete line of sight into all secondary-market activity, but that reality weighs in favor of strong SAR obligations and related monitoring expectations—not weaker ones. Where value can move quickly, pseudonymously, and through layered transaction paths, timely suspicious activity detection, escalation, and reporting become more important, not less. Treasury should therefore make clear that PPSIs must maintain monitoring, investigation, attribution, and record-retention capabilities sufficient to identify unusual patterns, investigate red flags, connect wallet-based activity to real-world actors where reasonably possible, and file useful SARs that support law enforcement even when full visibility is not available. The final rule should also ensure that PPSIs cannot avoid meaningful SAR responsibilities by pointing to technological limitations or fragmented transaction chains inherent in their own product design or distribution model.

Recordkeeping and Travel Rule

The proposed rule asks whether Recordkeeping and Travel Rule obligations for PPSIs and other financial institutions would be clearer if FinCEN codified a PPSI-specific Recordkeeping and Travel Rule.[28] In general, these rules require financial institutions to collect and retain identifying information about certain funds transfers and, in some cases, transmit that information to the next financial institution in the payment chain. FinCEN is seeking comment on whether a more tailored provision would improve clarity regarding the collection, retention, and transmission of required information in stablecoin transactions. ICBA supports codification if doing so would provide greater legal certainty,

clearer allocation of responsibilities, and more consistent supervisory and enforcement expectations across stablecoin transaction chains.

A PPSI-specific rule may be necessary because stablecoin activity often does not map neatly onto

[27] *Id.* at 18607.
[28] *Id.* at 18621.

traditional account-based payment models. Transaction flows may involve wallets, custodians, exchanges, omnibus arrangements, smart contracts, and layered intermediaries, making it difficult to determine who must collect, verify, retain, or transmit required information and at what point in the transaction chain. Those operational realities create real visibility and attribution challenges, but they do not justify weaker standards. To the contrary, where payment activity can move rapidly across channels with incomplete visibility into counterparties, beneficial ownership, transaction purpose, or downstream movement, Treasury should provide more precise rules—not fewer obligations.

Any PPSI-specific Recordkeeping and Travel Rule obligations should therefore make clear what information must be collected, when reliance on another intermediary is permissible, how responsibilities apply in primary- and secondary-market contexts, and what steps PPSIs must take whenever complete information is not immediately available. The final rule should not create a safe harbor for incomplete information or allow firms to cite technological limitations inherent in their product design as a reason to avoid core recordkeeping and transmission responsibilities. Instead, Treasury should use codification to strengthen enforceability, improve coordination among covered institutions, and ensure that stablecoin-related payment activity does not proceed under materially weaker transparency standards than comparable activity conducted through community banks.

OFAC Sanctions Compliance Program Requirements

OFAC is proposing a new part 502, entitled the "Permitted Payment Stablecoin Issuer Effective Sanctions Compliance Program Regulations," to implement the GENIUS Act's requirement that PPSIs maintain an effective sanctions compliance program.[29] ICBA supports Treasury's decision to establish a distinct OFAC framework for PPSIs because sanctions compliance cannot be treated as incidental to stablecoin activity. Given the speed, cross-border reach, transferability, and potential visibility gaps associated with stablecoin transactions, PPSIs should be subject to clear, enforceable sanctions expectations that are at least comparable to those that apply to community banks offering functionally similar payment services.

Effective Sanctions Compliance Program Requirements

The proposed rule would require PPSIs to adopt and maintain an effective sanctions compliance program and, consistent with OFAC's 2019 compliance framework,[30] would ground that requirement in five core elements: senior management and organizational commitment, risk assessment, internal controls, testing and auditing, and training.[31] ICBA supports this approach because those elements reflect the basic architecture of an effective, risk-based sanctions program and provide an appropriate foundation for bank-like payment activity conducted through stablecoin structures. At the same time, Treasury should make clear that these expectations must be operationally meaningful and enforceable. PPSIs should not be permitted to satisfy this requirement through a superficial or check-the-box

[29] *Id.* at 18613.
[30] A Framework for OFAC Compliance Commitments" (the "2019 Compliance Framework") to support the regulated public's development of effective sanctions compliance programs with guidance on tailoring risk-based principles to an organization's unique characteristics and sanctions risk exposure.
[31] GENIUS Act (2025) (codified at 12 U.S.C. §§ 5901–5916) (requiring effective sanctions programs); see also *Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions-Compliance Program Requirements*, (implementing that requirement consistent with OFAC's compliance framework).

program that lacks the governance, escalation procedures, technical controls, independent review, and staffing necessary to identify and address sanctions risk in practice. The final rule should preserve flexibility to tailor controls to a PPSI's size, complexity, and business model, but that flexibility should not result in materially weaker sanctions standards than those that apply to community banks offering functionally similar payment services.

Lawful Orders and Wallet or Account Identifiers

The proposed rule would require PPSIs to maintain sanctions compliance capabilities to comply with lawful orders and asks whether Treasury should further define that term, including by clarifying that an "account" may include a wallet address or other identifier used to identify a holder of a payment stablecoin.[32]

ICBA supports clarifying the scope of "lawful order" and agrees that Treasury should expressly recognize that, in the stablecoin context, relevant identifiers may extend beyond traditional account numbers to include wallet addresses and other identifiers that function as the operational equivalent of an account. If the final rule does not clearly recognize those identifiers, it could create uncertainty as to whether obligations tied to lawful orders apply as fully in digital-asset environments as they do in traditional banking, resulting in unnecessary ambiguity and risk. At the same time, Treasury should define these concepts carefully and in operational terms. A wallet address does not always map neatly to a single identifiable person, legal owner, or beneficial owner, and in some transaction structures multiple persons or intermediaries may interact with the same address or control related addresses.

The final rule should therefore make clear that identifying an address is not a substitute for reasonable efforts to identify the relevant customer or counterparty where such information is available or can be obtained. Treasury should also provide sufficient clarity regarding what systems, controls, and documentation PPSIs must maintain to implement lawful orders effectively, including where activity moves quickly across wallets or intermediaries and where limited visibility into downstream transfers may complicate blocking, freezing, or related actions. In ICBA's view, the purpose of clarification should be to strengthen enforceability and prevent evasion—not to narrow the reach of lawful orders or create a weaker standard for stablecoin activity than would apply to comparable payment activity conducted through community banks. That is particularly important because OFAC has recently reiterated the foundational sanctions principle that U.S. persons may not do indirectly what they cannot do directly. A PPSI therefore should not be permitted to rely on intermediaries, wallet structures, or secondary-market distribution arrangements to argue that sanctions-related obligations stop where direct privity ends. The final rule should make clear that firms remain responsible for maintaining controls reasonably designed to prevent sanctioned persons from accessing, using, or benefiting from stablecoin activity indirectly through another party or transaction layer.

Block, Freeze, and Reject Capabilities

The proposed rule would require PPSIs to maintain the technical capability to block, freeze, and reject transactions as necessary to comply with sanctions obligations and lawful orders under the GENIUS

[32] 91 Fed. Reg. at 18605.

Act.[33] ICBA strongly supports that requirement. Treasury should not dilute this core expectation simply because stablecoin activity may occur through novel technological architectures or fragmented transaction chains. On the contrary, the speed, cross-border reach, and transferability of stablecoins make effective intervention capabilities especially important. If value can move rapidly across wallets, intermediaries, smart contracts, or platforms with limited visibility into the identity of the transacting parties or the downstream destination of funds, then the need for prompt, enforceable blocking and freezing capabilities becomes more acute, not less.

ICBA recognizes that PPSIs may face technical and operational challenges in implementing these capabilities, including questions regarding wallet architecture, token design, control over smart contract functionality, the role of intermediaries, treatment of omnibus or custodial arrangements, and the extent to which an issuer can act effectively once tokens move into secondary-market circulation. But those challenges should not become a basis for weaker obligations or open-ended flexibility.

A firm that chooses to issue a bank-like payment instrument using technology that limits its ability to identify relevant actors or intervene when required should not be permitted to operate under a reduced sanctions standard because of that design choice. Treasury should instead require PPSIs to build products, governance, contractual arrangements, and compliance systems that support timely execution of block, freeze, and reject functions, and should provide sufficiently clear guidance regarding what constitutes an effective capability in different transaction environments. Any implementation flexibility should be narrow, operationally justified, and designed to support compliance—not to excuse gaps in enforceability, create uncertainty for counterparties and examiners, or allow stablecoin activity to proceed under materially weaker controls than those that apply to community banks offering functionally similar payment services. Recent OFAC enforcement underscores why this point matters: firms cannot structure around sanctions prohibitions by inserting another party into the transaction flow or by relying on formal distinctions that obscure the economic reality of an indirect dealing. The final rule should therefore make clear that PPSIs must retain sufficient practical control to stop, block, freeze, or reject transactions when required and may not invoke technical fragmentation, intermediary involvement, or secondary-market complexity as a basis to avoid sanctions responsibilities that would apply if the same activity occurred more directly.

Implementation Period, Guidance, and Effective Date

FinCEN and OFAC propose a 12-month effective date to allow PPSIs time to implement the required compliance systems and controls.[34] Treasury seeks comments on whether that timeline is realistic.

ICBA does not believe Treasury can assume that a 12-month implementation period will be realistic in all cases while significant aspects of the broader stablecoin regulatory framework remain unresolved. Whether that timeframe is workable will depend not only on the content of the final FinCEN and OFAC rules, but also on when Treasury and other agencies finalize related proposals governing supervision, prudential expectations, reserve treatment, operational controls, third-party arrangements, and other requirements that will shape how PPSIs and their bank partners must build compliant systems.

If those related obligations remain unsettled, a nominal 12-month period could prove illusory because

---

[33] *Id*. at 18620.
[34] *Id.*

firms would be forced to design governance, monitoring, reporting, sanctions, vendor-management, and technical controls without a stable regulatory baseline. That problem is especially acute here because the proposed rules contemplate new compliance capabilities for activity that may move rapidly across wallets, intermediaries, and secondary-market channels with limited visibility into counterparties or downstream transfers.

Treasury should therefore make clear that the implementation timeline will be measured against a sufficiently complete and coordinated final framework, not simply the publication date of one or two final rules in isolation. At a minimum, the effective date should not begin to run until the core compliance expectations are final and sufficiently clear to permit meaningful implementation, testing, and examiner alignment. If Treasury cannot provide that level of clarity at finalization, it should adopt a longer or staged implementation period rather than require firms and their bank counterparties to build upon an uncertain and potentially shifting standard.

Conclusion

ICBA supports Treasury's effort to establish a federal illicit-finance framework for PPSIs, but Treasury should not finalize a rule that allows bank-like payment activity to operate under weaker AML/CFT and sanctions standards than those that apply to community banks. A weaker framework would invite regulatory arbitrage, reduce law-enforcement visibility, and undermine competitive equity.

Treasury should adopt a final rule that imposes strong baseline obligations on all PPSIs, establishes clear reporting and recordkeeping requirements, and ensures coordinated supervision without diluting accountability. Innovation in payment technology does not justify weaker compliance, weaker supervision, or weaker safeguards.

ICBA appreciates the opportunity to comment on the proposed rule and looks forward to continued engagement with Treasury as this rulemaking proceeds.

Sincerely,

/s/

Rhonda Thomas-Whitley
Senior Vice President, Regulatory Counsel

/s/

Brian Laverdure, AAP
Senior Director, Digital Assets and Innovation Policy